REMARKS

Claims 1-22 are pending in the application. Claims 1, 7, 12 and 18 are amended. Claims 1 and 12 are still the only two independent claims. The claims have been rejected under 35 U.S.C. 112, First Paragraph, under 35 U.S.C. 112, Second Paragraph, under 35 U.S.C. 101, under 35 U.S.C. 102(b), and under 35 U.S.C. 103(a). Those rejections are respectfully traversed and reconsideration is requested.

Objection to the Drawings

Fig. 5C has been objected to as including vague and indefinite text. Accordingly, Fig. 5C has been amended to remove the text deemed vague and indefinite. Withdrawal of the objection is respectfully requested.

Rejections under 35 U.S.C. 112, First Paragraph

Claim 7 has been rejected under 35 U.S.C. 112, First Paragraph, as failing to comply with the enablement requirement.

Claim 7 is being amended to more precisely define the subject matter which Applicants consider to be their invention. As described in the Applicants' specification at page 12, line 25 through page 13, line 5, one or more predicates 585 may be used to implement security policy logic (e.g., predicates 585-n may detect a "network open" event followed by a "read disk drive" event). Likewise, a multi-event control predicate can be defined to prevent removal of files from a specific server, or being burned to a CD/DVD, etc. In addition, as explained at page 15, lines 5-11, the invention may count multiple predicate violations before asserting control over a user's network.

Claim 7 has thus been amended to more clearly refer to "asserting multiple policy violation predicates" before "indicating a risk of use outside of the security perimeter".

As such, the 35 U.S.C. 112, First Paragraph, rejection of Claim 7 is now believed to be overcome. Withdrawal of that rejection is respectfully requested.

As similar amendment is being made to Claim 18.

Rejections under 35 U.S.C. 112, Second Paragraph

Claims 12-22 have been rejected under 35 U.S.C. 112, Second Paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention.

The Office Action states on page 3 that no physical components are described in Claims 12-22; however, the claims actually recite numerous physical components. For example, independent system Claim 12 recites that a sensor is located in the operating system of a user client device. The client device is a data processor (computer) which is a physical component. Furthermore, Claim 12 now also requires a digital asset usage policy server. The policy server is also a computer, which is a physical component. See, *In re Stephen W. Comiskey*, No. 2006-1286, *23-24 (Fed. Cir. 2007).

Therefore, independent system Claim 12 recites multiple physical components and, thus, is not indefinite.

Dependent system Claims 13-22 inherently include at least the same physical components of Claim 12 and, thus, are also not indefinite.

As such, the 35 U.S.C. 112, Second Paragraph, rejections of Claims 12-22 are believed to be overcome. Withdrawal of the rejections is respectfully requested.

Rejections under 35 U.S.C. 101

Claims 12-22 have also been rejected under 35 U.S.C. 101, as being directed to non-statutory subject matter.

The basis for the rejections under 35 U.S.C. 101 of system Claims 12-22 is the same as basis for the rejections under 35 U.S.C. 112, Second Paragraph (i.e., lack of a physical component). Therefore, for the same reasons as presented above, the 35 U.S.C. 101 rejections of Claims 12-22 are believed to be overcome and withdrawal of rejections is respectfully requested.

Rejections under 35 U.S.C. 102(b)

Claims 1-3, 5, 8, 11-14, 16, 19, and 22 have been rejected under 35 U.S.C. 102(b) as being anticipated by Shear (U.S. 20010042043).

Before discussing the cited reference, a brief review of the Applicants' disclosure may be helpful without limiting the claims. The Applicants' disclosure is directed to a method and system for controlling access to digital assets in a data processing environment. Referring to Figs. 2 and 3, an agent process 300 runs within an operating system kernel within clients 102 and/or servers 104 in a network. The agent process 300 includes sensors 500 to detect and track atomic events 350, such as file, printing, clipboard, and I/O device operations.

The agent 300 reports atomic events 350 to an activity journaling process typically running on an activity journaling server 104-2, which processes atomic event data 350 and coalesces it into what are called aggregate events 360. Aggregate events 360 are detected when a certain predetermined combination of atomic events occurs. Each aggregate event 360 is, thus, composed of one or more atomic events 350 that conform to some predetermined pattern indicative of activity that should be monitored.

Predicates 370, 585 that define enforcement policies are then forwarded to the agent process 300. When the predicates 370, 585 detect a policy violation, steps are taken to enforce the policies, as represented by the predicates 370, 585, at the point of use, within a security perimeter defined within a network of data processors.

Applicants are submitting herewith amended claims 1 and 12 that are believed to better distinguish the invention. In particular, the claims now more positively recite the invention as including steps of (a) defining a security perimeter that includes two or more data processing devices, and (b) defining one or more policy violation predicates which are then (c) asserted when a risk of use of that digital asset occurs (i.e., by an end user) outside of the security perimeter.

It is believed that by emphasizing these features that indeed the Shear prior art is better distinguished. In particular, Shear is concerned with preventing access to stored media (such as a movie recorded on a DVD). Shear does provide a "software container" that enforces restrictions at the point of access to the media (not unlike the system described in Fig. 1 of Applicants' specification). However, Shear has no notion of optionally applying end user action policies based on attempted use of digital assets outside of a security perimeter as defined for a network of data processors.

More particularly, according to Applicants' claimed invention, the assertion of a policy violation predicate depends upon a proposed action to be taken with the digital assets. One example sequence of events described in connection with Fig. 6 at page 14, lines 11-26 of Applicants' specification detects a first sequence of atomic level events (i.e., a file copy to a USB device) in which case the copy action will be allowed with the asset, and another sequence of events (i.e., copying the asset to a CD) which will only be allowed if the user first documents a legitimate business purpose. Even if Shear's system is considered to be a protecting digital asset, it does not teach optionally applying a policy based on the result of detecting a sequence of events.

Shear does disclose a rights management arrangement for storage media. The arrangement allows for encrypted digital properties to be stored on the storage medium, such as a DVD, in a tamper-resistant "software container". Associated with the digital properties are rules relating to whether or how many times the digital properties may be copied. The rules may then be enforced by consumer appliances, such as DVD players or recorders.

However, Shear is not detecting when the sequence of events indicates a risk of use of the digital asset *outside of a security perimeter defined in a network of computers.*

Shear also does not teach or suggest *"aggregating multiple atomic level events to determine a combined event"* as recited in Claim 1. The Office Action cites paragraph [0188] of Shear as disclosing the above limitation; however, the cited paragraph merely makes reference to other "Shear patents", which do not appear to be specifically defined, and to elements of these "Shear patents" without describing them in detail. The cited paragraph merely states that "elements described in the Shear patent specifications include "... usage control in response to a combination of derived metering information and rules set by content providers." The terms "metering information" and "rules" that are supposedly combined are not defined, much less defined as being equivalent to the present application's atomic level events. Paragraph [0197] of Shear describes in slightly more detail the concept of usage control though the use of security, metering, and usage administration capabilities, but still fails to define "metering" as being equivalent to the combined atomic level events of the present application. If assumed to be defined as information relating to a user's amount of usage of a particular resource, the term "metering information" is not equivalent to an atomic level event, because "metering information" would be a sort of measurement, while an atomic level event is an occurrence or action that takes place. Furthermore, if given its plain meaning, the term "rules" are not equivalent to atomic level events because a rule is not an occurrence or action that takes place. Therefore, the disclosure of combining "metering information" and "rules" in order to control usage does not teach or suggest aggregating multiple atomic level events to determine a combined event.

Furthermore, because Shear does not teach or suggest aggregating multiple atomic level events to determine a combined event, Shear cannot teach or suggest *"asserting a policy violation predicate if at least one combined event has occurred"* as claimed in Claim 1. The Office Action cites paragraph [0193] of Shear as disclosing the above limitation; however, paragraph [0193] simply states that "elements described in the Shear patent specifications include ... local secure execution of control processes," which does not disclose or even suggest asserting a policy based on the occurrence of a combined event.

Therefore, Claim 1 is believed to be in condition for allowance for at least these reasons.

Independent Claim 12 is similar to Claim 1 and should be found in allowable condition for the same reasons as presented above for independent Claim 1.

Dependent Claims 2, 3, 5, 8, 11, 13, 14, 16, 19, and 22 are directly or indirectly dependent on independent Claims 1 or 12 and, thus, are novel and nonobvious over the cited art for at least the same reasons as presented above for independent Claims 1 and 12.

Furthermore, dependent Claims 2, 3, 5, 8, 11, 13, 14, 16, 19, and 22 recite further limitations that are neither taught nor suggested by the cited art. For example, Shear does not teach or suggest that a policy violation predicate (or detector) is implemented (or located) *"in an operating system kernel of the user client device"* as claimed in Claims 2 and 13. While Shear discloses that its secure node may support a general purpose operating system that has a kernel, Shear does not specifically disclose that policy violation predicates are implemented within the kernel of the operating system of a user client device.

As such, the 35 U.S.C. 102(b) rejections of Claims 1-3, 5, 8, 11-14, 16, 19, and 22 are believed to be overcome, and withdrawal of these rejections is respectfully requested.

Rejections under 35 U.S.C. 103(a)

Claims 6, 17, and 20 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Shear. Claim 9 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Shear in view of Danieli (U.S. Patent No. 6,510,513). Claims 4, 7, 10, 15, 18, and 21 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Shear in view of McCarty (U.S. Patent No. 5,666,411).

Dependent Claims 6, 17, and 20 are directly or indirectly dependent on independent Claims 1 or 12 and, thus, are novel and nonobvious over the cited art for at least the same reasons as presented above for independent Claims 1 and 12. As such, the 35 U.S.C. 103(a) rejections of Claims 6, 17, and 20 are believed to be overcome.

Dependent Claim 9 is directly dependent on independent Claim 1 and, thus, is novel and nonobvious over the cited art for at least the same reasons as presented above for independent Claim 1. As such, the 35 U.S.C. 103(a) rejection of Claim 9 is believed to be overcome.

Dependent Claims 4, 7, 10, 15, 18, and 21 are directly or indirectly dependent on independent Claims 1 or 12 and, thus, are novel and nonobvious over the cited art for at least the same reasons as presented above for independent Claims 1 and 12. As such, the 35 U.S.C. 103(a) rejections of Claims 4, 7, 10, 15, 18, and 21 are also believed to be overcome.

Information Disclosure Statement

A Supplemental Information Disclosure Statement (SIDS) is being filed concurrently herewith. Entry of the SIDS is respectfully requested.

CONCLUSION

In view of the above amendments and remarks, it is believed that all claims (Claims 1-22) are in condition for allowance, and it is respectfully requested that the application be passed to issue. If the Examiner feels that a telephone conference would expedite prosecution of this case, the Examiner is invited to call the undersigned.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By______________________________
David J. Thibodeau, Jr.
Registration No. 31,671
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133
Date: 10/1/01

Amendments to the Drawings

Replacement drawing for Fig. 5C is being submitted herewith to replace the originally filed drawing.

Attachment: Replacement Sheet
Annotated Marked-Up Drawing

InstantMessenger	FileRead, TCPIPInbound, TCPIPOutbound, ~~(other protocols???)~~	Similar to FileLeftThroughNetworkPort. Combines all interleaving FileReads with the network events. The application image name is one of those known to be used for instant Messanger. May place constraints on the ports.	Process
P2PApp	FileRead, TCPIPInbound, TCPIPOutbound, UDPInbound, UDPOutbound, IPSECInbound, IPSECOutbound	Constrain the application name to be one of those known to be a P2PApp. Multiple ports will be used; some or all of them may have constraints. May constrain the protocol per app or per instance. Similar to FileLeftThroughNetworkPort as concerns interleaved file reads.	Process
FTPFile	FileRead, FileWrite, ~~??? (~~TCPIPInbound, TCPIPOutbound	May want to split into two events, one for reading and one for writing. Constrain to the common FTP port, unless the app is known by name to be an FTP client. Like FileLeftThroughNetworkPort, look for interleaved reads and network events, or interleaved writes and network events.	Process
RemoteAccess	TCPIPInbound, TCPIPOutbound, UDPInbound, UDPOutbound, IPSECInbound, IPSECOutbound	Do not incorporate FileRead events. Several ports may be used. Look for known image names of remote apps.	Process

FIG. 5C